

Security Controls Assessment for Federal Information Systems

Census Software Process Improvement Program
September 11, 2008

Kevin Stine
Computer Security Division
National Institute of Standards and Technology

Agenda

- Introduction to NIST
- NIST Risk Management Framework
- Security Control Assessment Basics
- Security Control Assessment Process
- Summary

National Institute of Standards and Technology

NIST is a non-regulatory federal agency whose mission is...



To promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life

Computer Security Division

- A component within the Information Technology Lab (ITL) that provides standards and technology to protect information systems against threats to
 - the confidentiality of information,
 - the integrity of information and processes, and
 - the availability of information and services
- in order to build trust and confidence in IT systems



NIST Publications

Security Standards and Guidelines

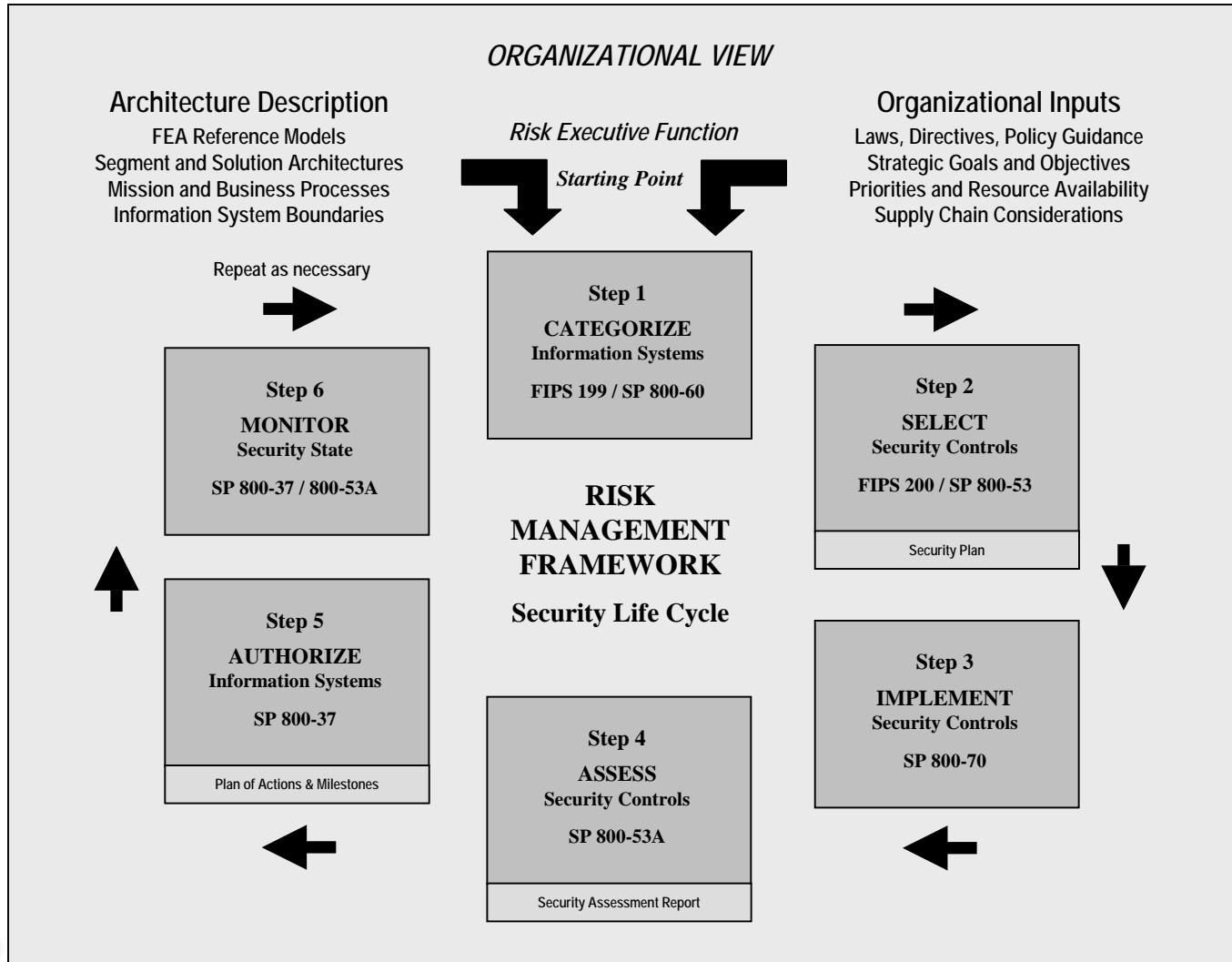
- Federal Information Processing Standards (FIPS)
 - Developed by NIST; Approved by Secretary of Commerce
 - Compulsory and binding for all federal agencies; not waivable
 - Examples: FIPS 197, FIPS 199, FIPS 200, FIPS 201
- Special Publications (SP; 800-series)
 - Series of information security publications of general interest to the security community
 - Examples: SP 800-18, SP 800-34, SP 800-53, SP 800-53A
- Other security-related publications
 - NIST Interagency Reports (NISTIRs) describe research and provide technical information of interest to a specialized audience

OMB on the Use of NIST Publications*

- For non-national security programs and information systems, agencies must follow NIST standard and guidelines
- For FY 2007 and beyond, agencies are required to use FIPS 200/NIST Special Publication 800-53 for the specification of security controls and NIST Special Publications 800-37 and 800-53A for the assessment of security control effectiveness

* OMB M-07-19, FY 2007 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management

NIST Risk Management Framework



Basics: What are Security Controls?

- The management, operational, and technical safeguards to protect the confidentiality, integrity, and availability of a system and its information.



Basics: Security Control Classes and Families

Management

- CA – Certification, Accreditation, and Security Assessments
- PL – Planning
- RA – Risk Assessment
- SA – System and Services Acquisition

Technical

- AC – Access Control
- AU – Audit and Accountability
- IA – Identification and Authentication
- SC – System and Communications Protection

Operational

- AT – Awareness and Training
- CM – Configuration Management
- CP – Contingency Planning
- IR – Incident Response
- MA – Maintenance
- MP – Media Protection
- PE – Physical and Environmental Protection
- PS – Personnel Security
- SI – System and Information Integrity

Basics: Security Control Baselines

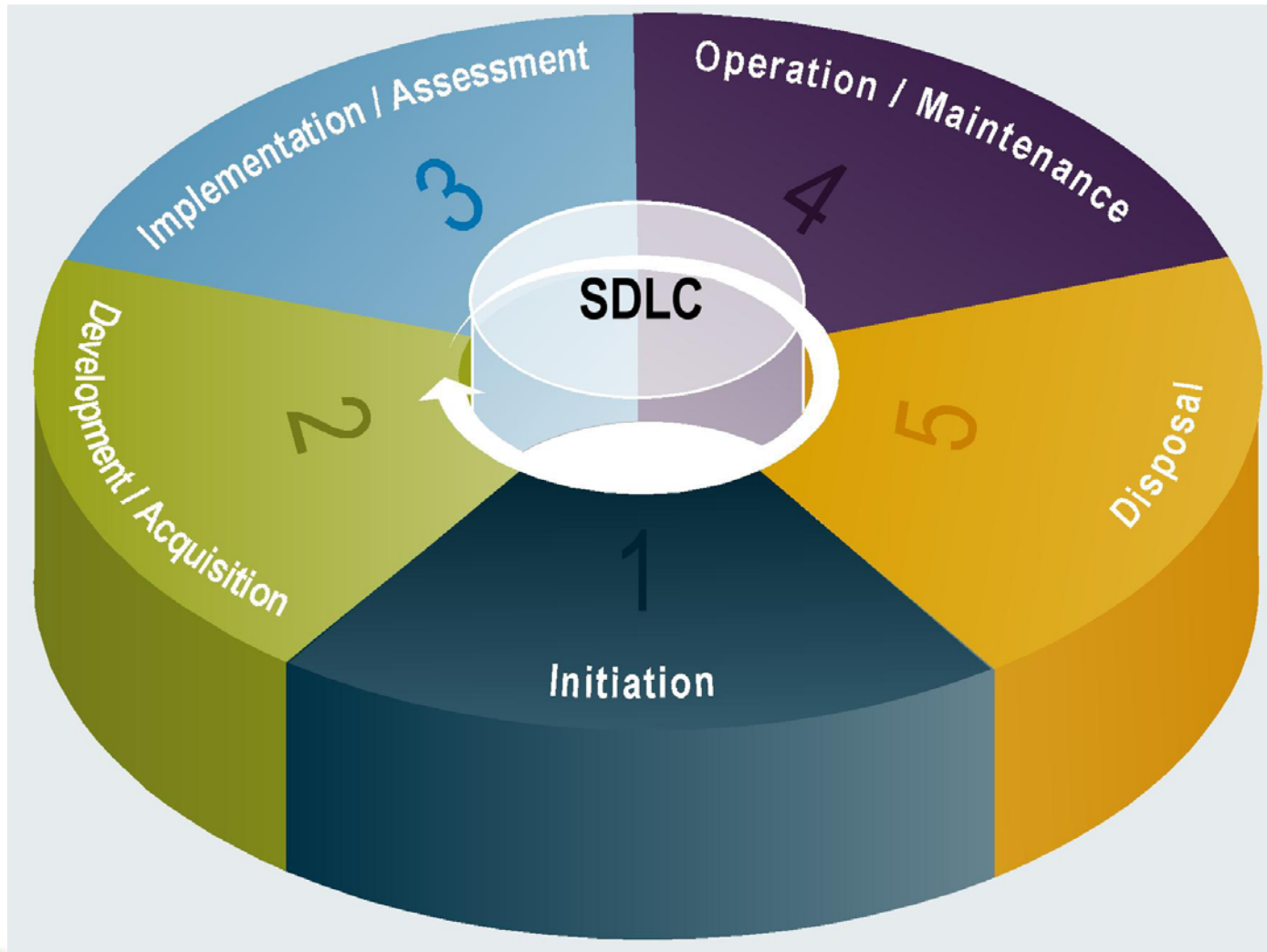
- Minimum security controls recommended for an information system based on its impact level (Low, Moderate, High)

CNTL NO.	Control Name	Control Baselines		
		LOW	MOD	HIGH
Access Control				
AC-1	Access Control Policy and Procedures	AC-1	AC-1	AC-1
AC-2	Account Management	AC-2	AC-2 (1) (2) (3) (4)	AC-2 (1) (2) (3) (4)
AC-3	Access Enforcement	AC-3	AC-3 (1)	AC-3 (1)
AC-4	Information Flow Enforcement	Not Selected	AC-4	AC-4
AC-5	Separation of Duties	Not Selected	AC-5	AC-5

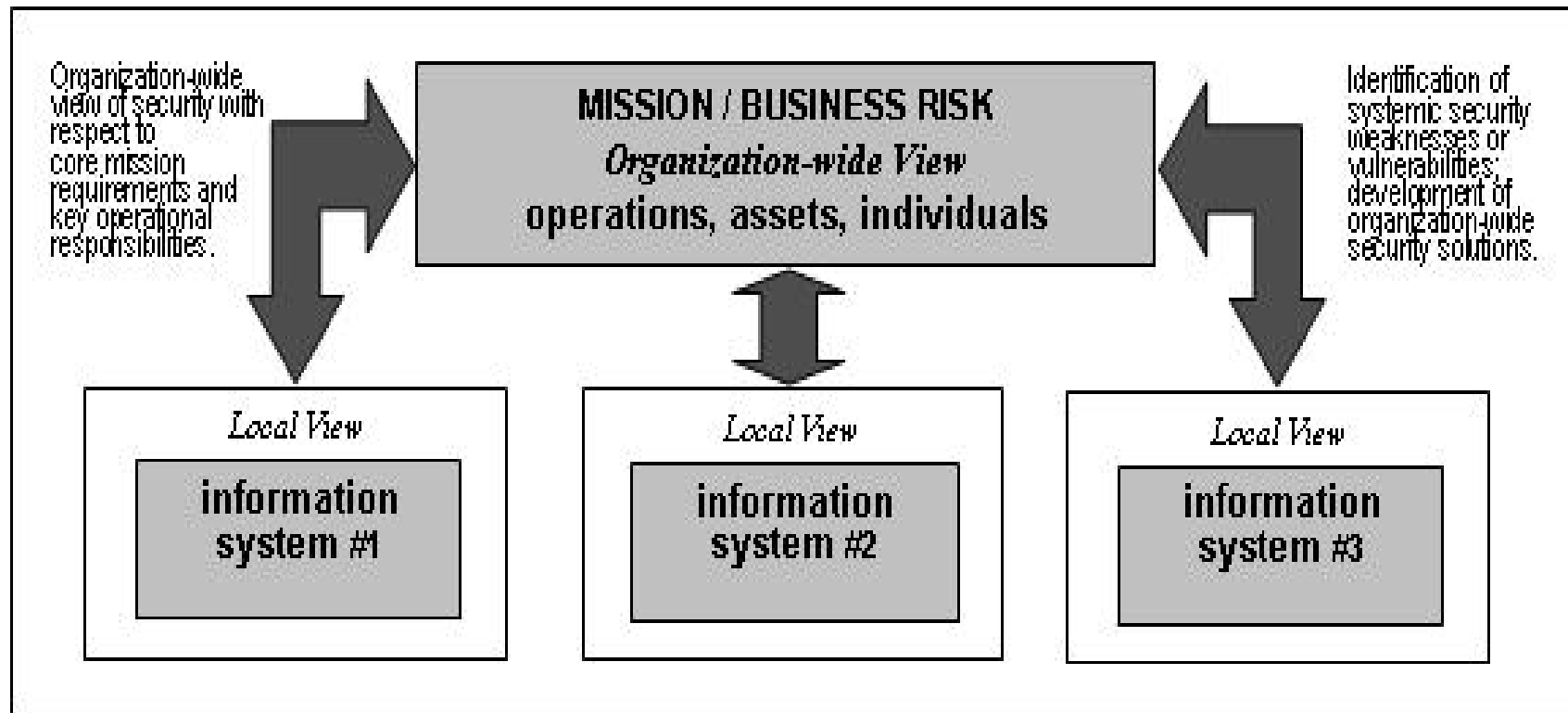
Basics: Security Control Assessments

- Principle vehicle used to verify that the implementers and operators of information systems are meeting their stated security goals and objectives
- Results of these assessments provide:
 - Evidence about the effectiveness of security controls;
 - An indication of the quality of the risk management processes employed within the organization; and
 - Information about the strengths and weaknesses of information systems supporting federal missions and applications.

Basics: Assessments within the SDLC



Basics: Organization-wide Strategy for Assessments



Basics: Security Controls About Assessments

CA-2	Security Assessments	L, M, H	The organization conducts an assessment of the security controls in the information system [Assignment: organization-defined frequency, at least annually] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.
CA-4	Security Certification	L, M, H	The organization conducts an assessment of the security controls in the information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.
CA-7	Continuous Monitoring	L, M, H	The organization monitors the security controls in the information system on an ongoing basis.

Basics: Who Conducts Assessments?

- System evaluators, certification agents/team, auditors, inspectors general, information system owners, information security personnel
- Assessor Independence
 - Identifies the degree to which the assessor is capable of conducting an impartial assessment of an information system.
 - An independent assessment of a security control's effectiveness must be performed for FIPS 199 Moderate and High impact systems when the assessment is supporting the system security certification.

Basics: Assurance for Security Control Effectiveness

- Compile evidence that controls are
 - Implemented correctly,
 - Operating as intended, and
 - Producing the desired outcome with respect to meeting the security requirements of the system
- Present this evidence in a manner decision makers are able to use to make informed, risk-based decisions
- The evidence to support assurance starts with the specification and implementation of the security controls, and is enhanced through the assessment of that implementation

Basics: Assessment Procedures

- A set of assessment objectives and an associated set of assessment methods and assessment objects.
 - Assessment Objectives – includes set of determination statements related to the security control under assessment
 - Assessment Objects – identify the specific items being assessed;
 - Specifications – document-based artifacts (e.g., policies, procedures, plans)
 - Mechanisms – hardware, software, or firmware safeguards (including physical protection devices)
 - Activities – action safeguards that involve people (e.g., monitoring network traffic, exercising a contingency plan)
 - Individuals – people applying the specifications, mechanisms, and activities

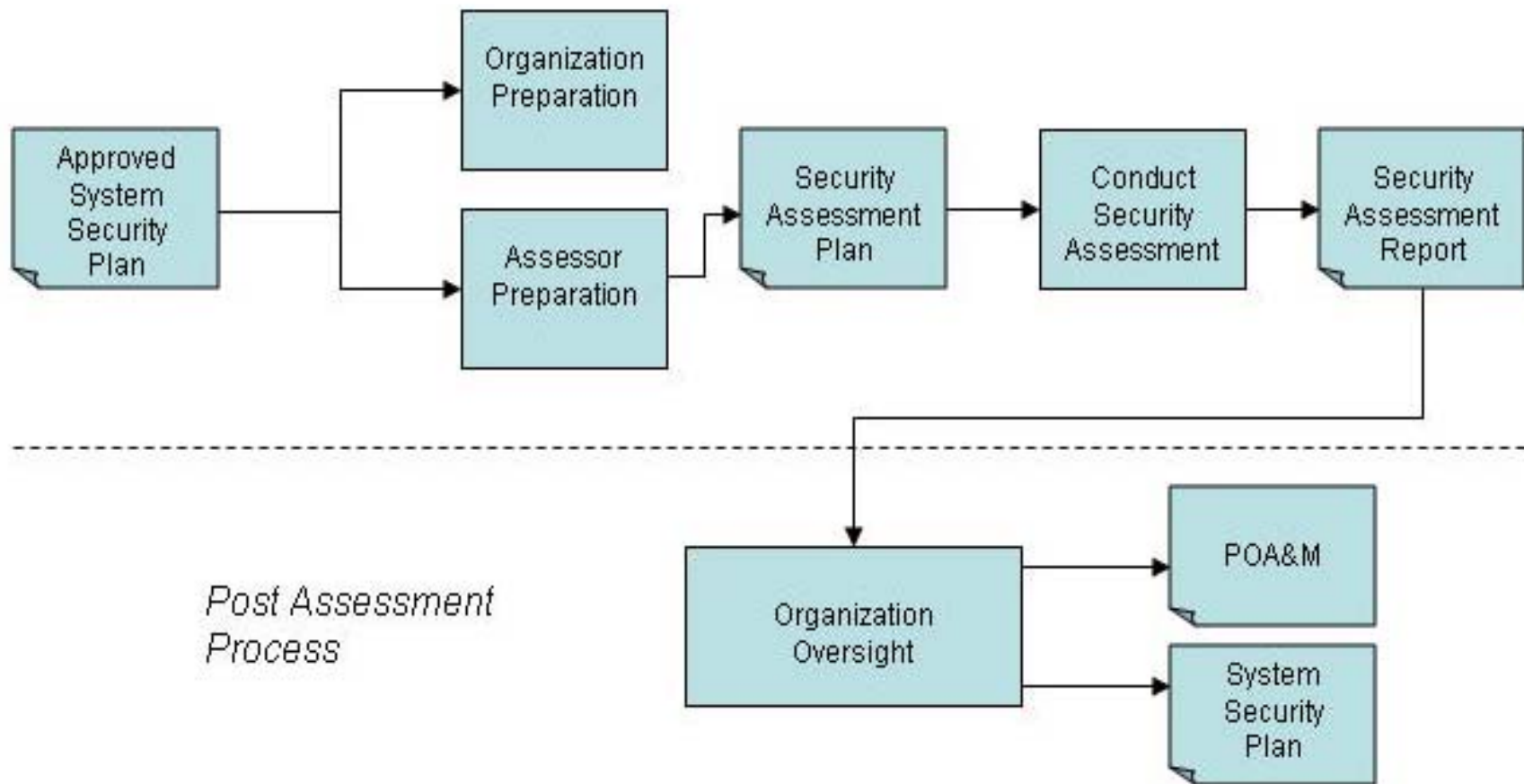
Basics: Assessment Procedures, cont

- Assessment Methods – define nature of the assessor actions;
 - Examine – review, inspect, observe, study, analyze
 - Interview – conduct discussions with individuals/groups
 - Test – exercising one or more assessment objects under specified conditions to compare actual with expected results
- Method Attributes
 - Depth – rigor of and level of detail (generalized, focused, detailed)
 - Coverage – scope or breadth (representative, specific, comprehensive)

Basics: Extended Assessment Procedures

- Applied to assessment as a whole
- Designed to work with and complement the assessment procedures
- Contribute to the grounds for confidence in the effectiveness of the security controls employed in the information system.
- Closely linked to the impact level of the information system and the assurance requirements in SP 800-53

Security Control Assessment Process



*Post Assessment
Process*

Process: Preparing for the Assessment

Organization	Assessor
Ensure assessment policies are in place and understood	Understand the organization's operations, and how the information system supports them
Ensure earlier NIST RMF steps have been completed , and received appropriate management oversight	Understand the system architecture and the security controls being assessed
Clearly define purpose and scope of assessment	Identify system personnel, and establish contacts needed to conduct the assessment
Notify, Communicate, and Allocate	Obtain necessary artifacts, including previous assessment results appropriate for reuse
Collect artifacts to provide to assessor	Meet with appropriate organization officials to ensure common understanding of assessment objectives, rigor, and scope
Establish processes to minimize ambiguity or misunderstandings between organization and assessor	Develop a security assessment plan

Process: Develop the Security Assessment Plan

- Provides the objectives for the Security Controls Assessment and a detailed roadmap of how to conduct the assessment
- Use SP 800-53A in conjunction with SP 800-53 (Security Controls Catalog)
- Assessors should work with organization to develop the plan
 - Determine the type of assessment (e.g., complete, partial)
 - Select appropriate procedures to assess the security controls
 - Tailor the assessment procedures to the specific operating environment
 - Assessment method and object considerations
 - Common security control-related considerations
 - Reuse of assessment evidence considerations
 - External information system considerations
 - System/platform and organization-related considerations

Process: Develop the Security Assessment Plan, cont

- Develop assessment procedures for
 - Organization-specific security controls
 - Additional assurance requirements
- Develop strategy for incorporating extended assessment procedures
- Optimize selected assessment procedures to ensure efficiency
- Finalize and obtain approval

Process: Conduct Assessment

- Execute Security Assessment Plan in accordance with agreed upon schedule and milestones
- Apply assessment methods to assessment objects, and compile/produce evidence necessary to make determination
 - Satisfied - assessment objective for the control has been met, producing a fully acceptable result
 - Other than Satisfied – evidence collected may indicate potential anomalies, or may be insufficient to make determination
- The final output and end result of the security controls assessment is the Security Assessment Report, one of the three key documents in the security accreditation package

Post Assessment Process: Organization Oversight

- System owner and organization officials review all findings of “other than satisfied”
 - Make risk-based remediation decisions based on severity/seriousness of finding
 - Document all decisions
- Update key documentation
 - System Security Plan with Risk Assessment
 - Update to reflect remediation actions, including risk-based acceptance
 - Plan of Actions and Milestones (POA&M)

Use of Automation to Support Assessments

- Information Security Automation Program (ISAP) and Security Content Automation Protocol (SCAP)
 - Support and complement the SP 800-53A approach for achieving consistent, cost-effective security control assessments
 - Improve automated application, verification, and reporting of product-specific security configurations
 - Achieve direct linkage, where appropriate, of the SP 800-53A assessment procedures to the SCAP automated testing of information system mechanisms and associated security configurations.

Use of Penetration Testing

- Controlled pen-testing should be considered as an additional tool to assess security controls
 - Enhance the organization's understanding of the system;
 - Uncover weaknesses in the system
 - Indicate the level of effort required of adversaries to breach the system safeguards.

Summary and Implementation Tips

- Rely on local IT security policies, procedures, and information security program for security control selection, implementation, and assessment details
- Reuse previous assessment results where possible
- Select only those assessment procedures that correspond to controls and enhancements in the approved security plan
- Procedures from 800-53A are exemplary – review, tailor, and supplement as necessary
- Security is fluid - periodic assessment of risk is necessary to ensure adequate security control coverage
- Communication is key – set expectations

Contact Information

Computer Security Division
National Institute of Standards and Technology
100 Bureau Drive, Mailstop 8930
Gaithersburg, MD USA 20899-8930

Kevin Stine
Kevin.Stine@nist.gov

CSD on the Web: <http://csrc.nist.gov>